CLAIMS

What is claimed is:

1. A method of security comprising the steps of:

a) enabling an electronic device to run a controlled application with an encrypted record containing a copied serial number and a first authorization level;

b) verifying said electronic device is correctly enabled; and

c) verifying said first authorization level is of sufficient authority to run said controlled application on said electronic device.

2. The method of security as described in Claim 1, wherein step a) comprises the steps of:

a1) fetching a serial number uniquely associated with said electronic device, said serial number located on said electronic device;

a2) copying said serial number, forming said copied serial number that is identical to said serial number;

a3) creating a record that contains said copied serial number and said first authorization level, said first authorization level previously assigned to said electronic device;

a4) encrypting said record, forming said encrypted record; and

a5) storing said encrypted record in said electronic device.

3. The method of security as described in Claim 2, wherein step b) comprises the steps of:

b1) locating said encrypted record;

b2) decrypting said encrypted record, if said encrypted record is located;

b3) reading said copied serial number from said encrypted record, if said encrypted record is successfully decrypted;

b4) fetching said serial number; and

b5) comparing said serial number and said copied serial number.

4. The method of security as described in Claim 3, wherein step b) comprises the further step of

executing said controlled application on said electronic device, said controlled application having controlled attributes;

5. The method as described in Claim 3, wherein said step c) comprises the steps of:

c1) reading said first authorization level from said encrypted record that is decrypted, if said serial number and said copied serial number match;

c2) comparing said first authorization level with a second authorization level assigned to said controlled application; and

c3) allowing access to said controlled attributes of said controlled application, if said first authorization level is of an equal or higher authorization level than said second authorization level.

6. The method as described in Claim 2, wherein step a) is performed with an enabler application, said enabler application enabling said electronic device to run applications having authorization levels equal to or lower than said first authorization level.

7. The method as described in Claim 6, comprising the further step of:

removing said enabler application from said electronic device after successfully completing step a).

8. The method as described in Claim 5, comprising the further step of:

aborting said application if any of the following conditions are met:

said encrypted record is not successfully located in step b1);

said encrypted record is not successfully decrypted in step b2);

said serial number and said copied serial number do not match in step b5); or

said first authorization level is of a lesser value than said second authorization level in step c2).

9. The method as described in Claim 5, comprising the further step of:

denying access to said controlled attributes of said controlled application if any of the following conditions are met:

said encrypted record is not successfully located in step b1);

said encrypted record is not successfully decrypted in step b2);

said serial number and said copied serial number do not match in step b5); or

said first authorization level is of a lesser value than said second authorization level in step c2).

10. The method as described in Claim 1, wherein said encrypted record is stored as a locked flash record in said electronic device.

11. The method as described in Claim 2, wherein said serial number is stored as a locked flash record in said electronic device.

12. The method as described in Claim 5, wherein said controlled application performs steps b) and c).

13. A method of security comprising the steps of:

a) executing an application on an electronic device, said application having controlled attributes;

b) locating an encrypted record that is stored in said electronic device, said encrypted record containing a copied serial number and a first authorization level;

c) decrypting said encrypted record, if said encrypted record is successfully located;

d) fetching a serial number, if said encrypted record is successfully decrypted, said serial number uniquely associated with said electronic device and located on said electronic device;

e) reading said copied serial number from said encrypted record that is decrypted, if said encrypted record is successfully decrypted;

f) comparing said serial number and said copied serial number;

g) reading said first authorization level from said encrypted record that is decrypted, if said serial number and said copied serial number match;

h) comparing said first authorization level with a second authorization level assigned to said application, said first authorization level previously assigned to said electronic device; and

i) allowing access to said controlled attributes of said application, if said first authorization level is of an equal or higher authorization level than said second authorization level.

14. The method as described in Claim 13, comprising the further steps of:

j) fetching said serial number;

k) copying said serial number, forming said copied serial number that is identical to said serial number;

l) creating a record containing said copied serial number and said first authorization level, said first authorization level previously assigned to said electronic device;

m) encrypting said record, forming said encrypted record; and

n) storing said encrypted record in said electronic device.

15. The method as described in Claim 14, wherein an enabler application performs steps j) through n) to enable said electronic device to run applications having authorization levels equal to or lower than said first authorization level.

16. The method as described in Claim 13, wherein said application performs steps b) through i).

17. The method as described in Claim 14, wherein the same encryption/decryption protocol is used in performing steps c) and m).

18. The method as described in Claim 13, comprising the further step of:

aborting said application if any of the following conditions are met:

said encrypted record is not successfully located in step b);

said encrypted record is not successfully decrypted in step c);

said serial number and said copied serial number do not match in step f); or

said first authorization level is of a lesser value than said second authorization level in step h).

19. The method as described in Claim 13, comprising the further step of:

denying access to said controlled attributes of said application if any of the following conditions are met:

said encrypted record is not successfully located in step b);

said encrypted record is not successfully decrypted in step c);

said serial number and said copied serial number do not match in step f); or

said first authorization level is of a lesser value than said second authorization level in step h).

20. A computer system comprising:

a bus;

a memory unit coupled to said bus; and

a processor coupled to said bus, said processor for executing a method of security comprising the steps of:

a) enabling an electronic device to run a controlled application with an encrypted record containing a copied serial number and a first authorization level;

b) verifying said electronic device is correctly enabled; and

c) verifying said first authorization level is of sufficient authority to run said controlled application on said electronic device.

21. The computer system as described in Claim 20, wherein step a) of said method comprises the steps of:

a1) fetching a serial number uniquely associated with said electronic device, said serial number located on said electronic device;

a2) copying said serial number, forming said copied serial number that is identical to said serial number;

a3) creating a record that contains said copied serial number and said first authorization level, said first authorization level previously assigned to said electronic device;

a4) encrypting said record, forming said encrypted record; and

a5) storing said encrypted record in said electronic device.

22. The computer system as described in Claim 21, wherein step b) of said method comprises the steps of:

b1) locating said encrypted record;

b2) decrypting said encrypted record, if said encrypted record is located;

b3) reading said copied serial number from said encrypted record, if said encrypted record is successfully decrypted;

b4) fetching said serial number; and

b5) comparing said serial number and said copied serial number.

23. The computer system as described in Claim 22, wherein step b) of said method comprises the further step of

executing said controlled application on said electronic device, said controlled application having controlled attributes;

24. The computer system as described in Claim 22, wherein said step c) of said method comprises the steps of:

c1) reading said first authorization level from said encrypted record that is decrypted, if said serial number and said copied serial number match;

c2) comparing said first authorization level with a second authorization level assigned to said controlled application; and

c3) allowing access to said controlled attributes of said controlled application, if said first authorization level is of an equal or higher authorization level than said second authorization level.

25. The computer system as described in Claim 21, wherein step a) of said method is performed with an enabler application, said enabler application enabling said electronic device
to run applications having authorization levels equal to or lower than said first authorization level.

26. The computer system as described in Claim 25, wherein said method comprises the further step of:

removing said enabler application from said electronic device after successfully completing step a).

27. The computer system as described in Claim 24, wherein said method comprises the further step of:

aborting said application if any of the following conditions are met:

said encrypted record is not successfully located in step b1);

said encrypted record is not successfully decrypted in step b2);

said serial number and said copied serial number do not match in step b5); or

said first authorization level is of a lesser value than said second authorization level in step c2).

28. The computer system as described in Claim 24, wherein said method comprises the further step of:

denying access to said controlled attributes of said controlled application if any of the following conditions are met:

said encrypted record is not successfully located in step b1);

said encrypted record is not successfully decrypted in step b2);

said serial number and said copied serial number do not match in step b5); or

said first authorization level is of a lesser value than said second authorization level in step c2).

29. The computer system as described in Claim 20, wherein said encrypted record in said method is stored as a locked flash record in said electronic device.

30. The computer system as described in Claim 21, wherein said serial number in said method is stored as a locked flash record in said electronic device.

31. The computer system as described in Claim 24, wherein said controlled application in said method performs steps b) and c).